U.S. DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF ADMIRAL JAMES M. LOY
ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION

Before the

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS, AND THE CENSUS
COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

May 6, 2003

Good afternoon, Mr. Chairman and Members of the Subcommittee. Thank you for the opportunity to appear before the Subcommittee on behalf of the Transportation Security Administration (TSA) to discuss how the use of information technology can strengthen transportation security. TSA was established under the Aviation and Transportation Security Act (ATSA) just weeks after the tragic events of September 11, 2001. Since then, TSA has worked diligently to deploy Federal screeners and explosives detection systems at more than 429 airports across the country, dramatically expand the Federal Air Marshal (FAM) program, and enhance perimeter security at airports.

Now, having met the initial deadlines of ATSA, we are expanding our security efforts in other modes of transportation and finding ways to continually improve aviation security. One of the most promising opportunities for improving both efficiency and effectiveness in aviation security is to make greater use of information technology and risk analysis tools. Information technology can play a key role in protecting citizens from terrorist threats while protecting their privacy. This hearing is an important forum for developing a shared understanding that security and privacy are complementary, not conflicting, goals.

Currently, airlines operate the Computer Assisted Passenger Prescreening program (CAPPS) to identify passengers for enhanced screening before those passengers are permitted to board a commercial aircraft. In ATSA, Congress directed TSA to ensure that CAPPS or any successor system is used to evaluate all passengers before they board an aircraft and to include procedures to ensure that individuals selected by the system and their carry-on and checked baggage are adequately screened. As a result, TSA is developing an enhanced Computer Assisted Passenger Prescreening program (CAPPS II), which will far more effectively identify passengers that may be a risk to the aviation system.

The purpose of CAPPS II is to identify foreign terrorists and those with links to foreign terrorists that pose a threat to civil aviation security. CAPPS II also will allow TSA to

make more efficient use of screener resources by using dynamic intelligence information to select passengers for enhanced screening.

CAPPS II will be a limited, automated screening tool that will be operated under the direction of TSA and that will form a critical element in our strategy of providing overlapping layers of security to protect aviation from curbside to cockpit. Passenger pre-screening under CAPPS II is an essential component of our system-of-systems approach to aviation security.

CAPPS II will establish a more standardized risk assessment system, dramatically reducing what some travelers view as arbitrary selections of passengers for enhanced screening at airport security checkpoints. Indeed, by using this tool to focus screeners' efforts on passengers who appear to pose a heightened risk, much of the additional screening that is now performed may be eliminated. At present, under CAPPS, some 15 percent of passengers traveling within, through, or out of the U.S. undergo enhanced screening. Under CAPPS II, we expect that percentage to drop significantly, thus expediting travel for many passengers without compromising security.

CAPPS II will reduce much of the current confusion involving persons with similar names. Public trust and confidence in the security of air travel will increase with a more robust and fully audited pre-screening system. Implementation of CAPPS II also will relieve air carriers of the financial burden of operating the current CAPPS system, a cost airlines estimate at over $150 million annually.

In all we do, TSA strives to provide world-class security and world-class customer service. We cannot be successful in serving our customers without taking great strides to protect their privacy. TSA is mindful that privacy protections must be built into the CAPPS II system from its very foundation. We have been working with Congress and stakeholders in the privacy and civil liberties communities, and have made good progress toward that end. As Secretary Ridge has stated, we will not implement CAPPS II until the Department of Homeland Security's chief privacy officer has reviewed and approved the privacy protections in the program. I am pleased to report that the Department's new privacy officer, Ms. Nuala O'Connor Kelly, has already begun her review of CAPPS II. Under the E-Government Act, TSA is working to finalize its CAPPS II business case, which will detail how privacy and security are built into the system. TSA also will conduct a Privacy Impact Assessment.

Essentially, CAPPS II will be a passive system that produces a general indication of the level of terrorist risk each airline passenger might pose to civil aviation security. It will be activated by a traveler's airline reservation request. Airlines will ask passengers for specific reservation information that will include a passenger's full name, plus other identifiers including date of birth, home address, and home phone number. Passengers will not be asked to provide social security numbers, and TSA will not look at credit worthiness.

The CAPPS II process will then authenticate each passenger's identity through publicly and commercially available databases. Once a passenger's identity is authenticated and the passenger's information is run against terrorist or other appropriate Federal government systems, an aggregate numerical threat score will be generated that TSA will use to determine which passengers should proceed through the ordinary screening process and which passengers should be asked to submit to a somewhat more thorough screening. In extremely rare cases, the system may identify an individual who is a known foreign terrorist or the associate of a known foreign terrorist. In such a case, law enforcement authorities would be notified and given the opportunity to take appropriate action.

The entire risk assessment process will be conducted in less than five seconds. It is important to stress that TSA will rarely see the public-source information that is checked to authenticate passenger identity. The exception may be in the extremely rare case of passengers who are positively identified as known terrorists or associates of known terrorists. In such a case, the Federal government would need this information for enforcement purposes.

The CAPPS II process will allow the vast majority of passengers to simply go through ordinary screening. Fewer passengers will be subject to enhanced screening under CAPPS II, and this will lead to shorter lines. CAPPS II may be compared to an electronic lock protecting a secured area. You must identify yourself and satisfy the system before you are allowed entry. The system's algorithms will be designed to confirm passenger identity information, identify known and unknown foreign terrorists, and recognize connections to known terrorist-related activities or individuals.

CAPPS II is a passenger-screening tool only. It will not ingest or store large quantities of data. Very importantly, CAPPS II is not data mining in that it will not explore databases to extract information to identify patterns of behavior among travelers.

CAPPS II will operate under a stringent privacy protection protocol being developed through discussions with privacy groups, both in the U.S. and internationally, with Congress, and with the public. Strict firewalls and access rules will protect a traveler's information from inappropriate use, sharing, or disclosure. CAPPS II will not retain data on U.S. passengers that are permitted to fly. Once travel is completed, CAPPS II records on these passengers will be purged.

I want to recognize the valuable contributions the privacy community has made in the development of this system. In March, TSA held a three-day privacy summit that was attended by many leading privacy experts. The discussion was frank. TSA listened carefully to all views, and we are giving these views full consideration as decisions about CAPPS II are made. In the weeks ahead, we are holding public meetings around the country to get the view of as many people as possible so that our privacy protections respond to the concerns and have the support of most Americans. Briefings for officials, privacy advocates, and opinion leaders have been and will continue to be conducted on a regular, on-going basis. We are reviewing comments submitted in response to our

Federal Register notice and will issue a new notice based on comments received. TSA, in conjunction with the State Department, is also working with the European Commission to ensure that international privacy concerns are fully addressed.

Based on TSA's outreach to the privacy community and the public, additional privacy measures are being incorporated into CAPPS II. CAPPS II will minimize the amount of information on travelers that ever comes into the system, using only the information that is necessary to conduct an identity authentication and risk assessment. The base information needed to operate CAPPS II will be provided by passengers themselves. The CAPPS II authentication function will be conducted for the most part outside government databases using commercially available data, and very importantly, data in those systems will not be viewed by TSA. Employees of commercial data companies assisting with the authentication process will never directly view or acquire records of traveler personal information from TSA. A system of firewalls will prevent these companies from ever directly using or retaining personal information.

TSA wants travelers to fully understand at the outset how information they provide will be used. To that end, we are developing procedures consistent with the Privacy Act to provide timely notification to individual airline ticket purchasers of the purpose for which we are obtaining information about them and the need for such information.

TSA will maintain a policy of openness and public accountability. When a passenger feels that he or she is being singled out for heightened scrutiny, complaint procedures will enable that passenger to bring a grievance to the attention of TSA. TSA is committed to affording any aggrieved passenger prompt access to appropriate redress or assistance.

It will not always be possible to inform a passenger of the reason for any additional screening that may be performed. However, TSA's Passenger Advocate will be empowered to look into any issues or concerns raised by a passenger.

Security is a primary concern for TSA in the construction of the CAPPS II program. TSA takes the responsibility for handling personal data very seriously and will use the best technology to ensure that data is handled properly and that inadvertent disclosures do not occur. To that end, CAPPS II will be a policy and security based system with real-time auditing. Access to the system will be limited to those with an appropriate need, and the system will monitor and identify precisely who accesses the system, when it was accessed, and for how long. Data input will be validated to ensure that it is correct, authorized, and appropriate in light of applicable restrictions. The CAPPS II design will ensure that data is securely transferred between systems and end-users.

We are also working aggressively across the Department to ensure that CAPPS II technology is appropriately leveraged with other DHS investments in screening technology. This Department-wide review and planning will help achieve a key DHS goal of preventing unnecessary duplication and wasted taxpayer dollars.

The CAPPS II system is still under development. We are now testing the technology to ensure that it functions properly, but we are not piloting the system itself. Passenger data is not being transferred or processed. TSA expects to have CAPPS II fully implemented by the summer of 2004. I look forward to working with this Subcommittee in the months ahead as we develop CAPPS II, to realize the efficiency and effectiveness it offers in improving security while protecting the privacy interests of travelers.

Thank you for the opportunity to appear before your Subcommittee. I would be pleased to answer any questions you may have.